Minimum Distance of Concatenated Conjugate Codes for Cryptography and Quantum Error Correction

Mitsuru Hamada

***Abstract*— A polynomial construction of error-correcting codes for secure and reliable information transmission is presented. The constructed codes are essentially Calderbank-Shor-Steane (CSS) quantum codes, and hence are also useful for quantum error correction. The asymptotic relative minimum distance of these codes is evaluated, and shown to be larger than that of the codes constructed by Chen, Ling and Xing (2001) for a wide range. Known lower bounds on the minimum distance of enlarged CSS quantum codes are also improved.**

***Index Terms*— conjugate code pairs, quotient codes, concatenation, minimum distance, geometric Goppa codes.**

I. Introduction

A polynomial construction of error-correcting codes for secure and reliable information transmission is presented. The codes to be given are essentially Calderbank-Shor-Steane (CSS) codes, originally proposed as quantum error-correcting codes [1], [2]. We describe our result using the term conjugate code pairs, which is almost a synonym for CSS codes. This term and a related one 'quotient codes' [3] were coined by the present author so that the design issue of this class of codes would be more accessible to those unfamiliar with the formalism of quantum theory. These notions were defined without referring to Hilbert spaces but in terms of familiar finite fields or additive groups. In particular, we emphasize the next respect. In some applications of CSS codes such as cryptography, we need only classical information processing, not quantum one. For example, in a well-known application to quantum key distribution [4], we need quantum devices only for modulation. For details on the backgrounds, see [5, Section 1] and references therein.

A conjugate code pair is a pair of linear codes (C_1, C_2) satisfying the condition $C_2^\perp \leq C_1$, where $C^\perp$ denotes the dual of C, and by $B \leq C$, we mean B is a subgroup of an additive group C. In a recent paper [5], a method for concatenating conjugate code pairs was proposed. In that paper, the performance was analyzed of conjugate code pairs (C_1, C_2) such that both C_1 and C_2 (more precisely, quotient codes $C_1/C_2^\perp$ and $C_2/C_1^\perp$) are efficiently decodable.

While the primary performance measure of codes, i.e., the probability of successful decoding is evaluated in [5], [6], the minimum distance of concatenated conjugate codes will be investigated in the present work. The main result of this work (Theorem 2) parallels a known lower bound [7] to the largest minimum distance of classical constructible codes to some extent, and clarifies a relation to known lower bounds on CSS codes [8], [9].

The polynomial constructibility of classical codes was formulated and argued in [7], [10], [11] with the criterion of minimum distance employed. This problem formulation was brought into the realm of quantum coding in [12], which was followed by several works [8], [9], [13]. In particular, the CSS codes in [8] are worth mentioning, since the construction of concatenated conjugate codes in [5] includes those in [8] as a special case. We will evaluate the asymptotic relative minimum distance of concatenated conjugate codes in [5] to show that the general approach of [5] leads to improvements on codes in [8], [13] for wide ranges in terms of minimum distance.

This paper is organized as follows. In Section II, we give the definitions of quotient codes and conjugate codes. In Section III, we see how a metric can be induced on a quotient space from a metric on the original space. A basic lemma on the minimum distance of concatenated conjugate codes is presented in Section IV, and a general lower bound on the minimum distance is given in Sections V. Restricted but more concrete bounds are derived from the general one in Sections VI and VII to show improvements in Section VIII. Section IX contains a summary. Two appendices are given. One is to present a Zyablov-type bound that can be achieved by concatenated conjugate codes of simple structure, though their minimum distance is not as large as that presented in Section V. The other contains proofs of statements on enlarged CSS codes.

II. Quotient Codes and Conjugate Codes

We fix a finite field $\mathbb{F}_q$ of q elements, and construct codes over $\mathbb{F}_q$. We retain the notation of [5] in this paper.

An $[[n, k]]$ *quotient code* over $\mathbb{F}_q$ is an additive quotient group C/B with $B \leq C \leq \mathbb{F}_q^n$ and $k = \log_q |C|/|B|$. This double bracket notation should not to be confused with the conventional one where the code C is referred to as an $[n, k_1]$ code if $k_1 = \log_q |C|$. In the standard scenario of quotient codes [14], [3], a message is encoded into a 'code-coset' $c \in C/B$ (rather than a codeword), a word w in c is chosen randomly, and then w is sent over a channel that may be wiretapped.

An $[[n, k]]$ *conjugate code pair* is a pair (C_1, C_2) consisting of an $[n, k_1]$ linear code C_1 and an $[n, k_2]$ linear code C_2 satisfying

$$C_2^\perp \leq C_1 \tag{1}$$

and $k = k_1 + k_2 - n$. The rate of this pair, or of the quotient code $C_1/C_2^\perp$ (or $C_2/C_1^\perp$), is k/n. If the minimum distance

of an $[[n,k]]$ quotient code $C_1/C_2^\perp$, which is denoted by $\mathsf{d}_{C_2^\perp}(C_1)$ and defined in the next section, is d, then it is called an $[[n,k,d]]$ quotient code. If the minimum distance of an $[[n,k]]$ quotient code is not smaller than d, it is referred to as an $[[n,k,\geq d]]$ quotient code. An $[[n,k]]$ conjugate code pair (C_1,C_2) with $d=\min\{\mathsf{d}_{C_2^\perp}(C_1),\mathsf{d}_{C_1^\perp}(C_2)\}$ is called an $[[n,k,d]]$ conjugate code pair.

We want a conjugate code pair (C_1,C_2) such that both $C_1/C_2^\perp$ and $C_2/C_1^\perp$ are good. In this paper, the measure of goodness is the minimum distance of codes.

III. Metrics for Quotient Spaces

To evaluate minimum distance, we use the metric naturally induced in a quotient space. For generality, we begin with spaces of the form $\mathcal{V}=\mathcal{Z}/B$, where $B\leq\mathcal{Z}$ are finite additive groups. Given a non-negative function W on $\mathcal{Z}$, a function D on $\mathcal{Z}\times\mathcal{Z}$ defined by $\mathsf{D}(x,y)=\mathsf{W}(y-x)$ is a metric if W satisfies (i) triangle inequality $\mathsf{W}(x+y)\geq\mathsf{W}(x)+\mathsf{W}(y)$, $x,y\in\mathcal{Z}$, (ii) $\mathsf{W}(x)=0$ if and only if x is zero, and (iii) $\mathsf{W}(x)=\mathsf{W}(-x)$. We have the following lemma, which was mentioned in an expository paper of the present author [3, Appendix, A.3].

Lemma 1: Given a function W on $\mathcal{Z}$, define $\mathsf{W}_B(\widetilde{x})=\min_{x\in\widetilde{x}}\mathsf{W}_B(x)$ for $\widetilde{x}\in\mathcal{Z}/B$. Then, whichever of properties (i), (ii) and (iii) W has, W_B inherits the same properties from W.

The easy proof omitted in [3] is included below.

Proof of Lemma 1. Given $\widetilde{x},\widetilde{y}\in\mathcal{Z}/B$, let x and y attain the minimum of $\min_{x\in\widetilde{x}}\mathsf{W}(\widetilde{x})$ and that of $\min_{y\in\widetilde{y}}\mathsf{W}(\widetilde{y})$, respectively. Then,

$$\begin{aligned}\mathsf{W}_B(\widetilde{x})+\mathsf{W}_B(\widetilde{y}) &= \mathsf{W}(x)+\mathsf{W}(y)\\ &\geq \mathsf{W}(x+y)\\ &\geq \min_{z\in\widetilde{x+y}}\mathsf{W}(z)\\ &= \mathsf{W}_B(\widetilde{x+y})\end{aligned}$$

where $\widetilde{x+y}=\widetilde{x}+\widetilde{y}\in\mathcal{Z}/B$. This prove the statement on (i). That on (ii) is trivial. To see that on (iii), it is enough to notice that when z runs through $\widetilde{x}=x+B$, $-z$ runs through $-x-B=-x+B=-\widetilde{x}$. □

The lemma is, of course, applicable to the Hamming weight, denoted by w, on the direct sum $\mathbb{F}^n$ of n copies of an additive group $\mathbb{F}$. Namely, the quotient space $\mathbb{F}^n/B$ is endowed with the weight w_B, defined by $\mathsf{w}_B(\widetilde{x})=\min_{x\in\widetilde{x}}\mathsf{w}(x)$ for $\widetilde{x}\in\mathbb{F}^n/B$, and the distance $\mathsf{d}_B(x,y)=\mathsf{w}_B(y-x)$. We write $\mathsf{d}_B(C)$ for the minimum distance of a quotient code C/B. Namely,

$$\begin{aligned}\mathsf{d}_B(C) &= \min\{\mathsf{d}_B(\widetilde{x},\widetilde{y})\mid\widetilde{x},\widetilde{y}\in C/B,\,\widetilde{x}\neq\widetilde{y}\}\\ &= \min\{\mathsf{w}_B(\widetilde{x})\mid\widetilde{x}\in C/B,\,\widetilde{x}\neq B\}\\ &= \mathsf{w}(C\setminus B)\end{aligned}\tag{2}$$

where, for $A\subseteq\mathbb{F}^n$,

$$\mathsf{w}(A)=\min\{\mathsf{w}(x)\mid x\in A\}.$$

IV. Minimum Distance for Concatenated Codes

We will evaluate the minimum distances of $L_1/\overline{L_2^\perp}$ and $L_2/L_1^\perp$ for $\underline{L_1}=\pi_1(D_1)+\overline{C_2^\perp}$ and $L_2=[\pi_1(D_2^\perp)+\overline{C_2^\perp}]^\perp=\pi_2(D_2)+\overline{C_1^\perp}$. The pair (L_1,L_2) is the *concatenated conjugate code pair* made of inner code pairs $(C_1^{(i)},C_2^{(i)})$, $i=1,\ldots,N$, over $\mathbb{F}_q$ and an outer code pair (D_1,D_2) over $\mathbb{F}_{q^k}$ [5]. For most part, we describe the argument only for $L_1/\overline{L_2^\perp}$, the other case being obvious by symmetry.

We recall how the quotient code $L_1/\overline{L_2^\perp}$ was defined in [5]. In short, $\overline{C_2^\perp}=\bigoplus_{i=1}^N C_2^{(i)\perp}$, where $(C_1^{(i)},C_2^{(i)})$ is the i-th inner $[[n^{(i)},k]]$ conjugate code pair, and $L_1/\overline{C_2^\perp}$ is obtained by mapping each symbol of words of D_1 to $C_1^{(i)}/C_2^{(i)\perp}$ as $\widetilde{\pi_1^{(i)}}:\mathbb{F}_{q^k}\ni x_i\mapsto\pi_1^{(i)}(x_i)+C_2^{(i)\perp}$, where $\pi_1^{(i)}$ is the one-to-one linear map from $\mathbb{F}_{q^k}$ onto a set of coset representatives of $C_1^{(i)}/C_2^{(i)\perp}$. The overall effect of $\widetilde{\pi_1^{(i)}}$, $1\leq i\leq N$, is represented by the map

$$\widetilde{\pi_1}:\mathbb{F}_{q^k}^N\ni x\mapsto\pi_1(x)+\overline{C_2^\perp},\tag{3}$$

where $\pi_1(x)=\left(\pi_1^{(1)}(x_1)\cdots\pi_1^{(N)}(x_N)\right)\in\mathbb{F}_q^{\sum_i n^{(i)}}$ for $x=(x_1,\ldots,x_N)$ [5].

With the conjugate code pair (D_1,D_2), or equivalently, quotient code $D_1/D_2^\perp$ over $\mathbb{F}_{q^k}$ given, we apply $\widetilde{\pi_1}$ to D_1 and $D_2^\perp$ to have $[\pi_1(D_1)+\overline{C_2^\perp}]/[\pi_1(D_2^\perp)+\overline{C_2^\perp}]=L_1/L_2^\perp$. The case where $(C_1^{(i)},C_2^{(i)})$, $i=1,\ldots,N$, are all equal to a fixed $[[n,k]]$ conjugate code pair (C_1,C_2) would be the most practical. In this case, the resulting quotient code $L_1/L_2^\perp$ has the parameters $[[nN,kK]]$, and is called the *concatenation* of $C_1/C_2^\perp$ and $D_1/D_2^\perp$. The corresponding conjugate code pair (L_1,L_2) is called the *concatenation* of (inner) conjugate code pair (C_1,C_2) and and (outer) conjugate code pair (D_1,D_2). A fundamental fact established in [5] is the following theorem, where π_1 and π_2 are closely related by dual bases of $\mathbb{F}_{q^k}$.

Theorem 1: [5]

$$[\pi_1(D_2^\perp)+\overline{C_2^\perp}]^\perp=\pi_2(D_2)+\overline{C_1^\perp},$$
$$[\pi_2(D_1^\perp)+\overline{C_1^\perp}]^\perp=\pi_1(D_1)+\overline{C_2^\perp}.$$

Here, an underlying idea that has brought about the results of the present work is explained. The point is that both L_1 and $L_2^\perp$ have the subspace $\overline{C_2^\perp}$, and we encode no information into $\overline{C_2^\perp}$. Namely, we encode a message into a 'code-coset' of the form $u+L_2^\perp\in L_1/L_2^\perp$, which can be written in the form $\bigcup_v(v+\overline{C_2^\perp})$ since we have $\overline{C_2^\perp}\leq L_2^\perp$ $(\leq L_1)$. This means there is no harm in dealing with the quotient space $\mathbb{F}_q^{N_\circ}/\overline{C_2^\perp}$, where $N_\circ=\sum_{i=1}^N n^{(i)}$, in place of $\mathbb{F}_q^{N_\circ}$, which is to be dealt with when the conventional concatenated codes are in question. This is possible because each space $\mathbb{F}_q^{n^{(i)}}/C_2^{(i)\perp}$ is endowed with the weight $\mathsf{w}_{C_2^{(i)\perp}}$ as described in Section III.

Lemma 2: The minimum distance of the quotient code $L_1/L_2^\perp=[\pi_1(D_1)+\overline{C_2^\perp}]/[\pi_1(D_2^\perp)+\overline{C_2^\perp}]$ is not smaller than d_1d', where $d_1=\min_{1\leq i\leq N}\mathsf{d}_{C_2^{(i)\perp}}(C_1^{(i)})$ and $d'=\mathsf{d}_{D_2^\perp}(D_1)$. The minimum distance of the quotient code $L_2/L_1^\perp=[\pi_2(D_2)+\overline{C_1^\perp}]/[\pi_2(D_1^\perp)+\overline{C_1^\perp}]$ is not smaller than d_2d'', where $d_2=\min_{1\leq i\leq N}\mathsf{d}_{C_1^{(i)\perp}}(C_2^{(i)})$ and $d''=\mathsf{d}_{D_1^\perp}(D_2)$.

Remark. From the proofs below, we see the minimum distance of $L_1/L_2^\perp$ equals dd' if all the inner codes $C_1^{(i)}/C_2^{(i)\perp}$ have minimum distance d. □

Proof 1. By symmetry, it is enough to show the first statement. We see this easily working with $\mathsf{d}_{\overline{C_2^\perp}}$. In fact, for any $x \in D_1 \setminus D_2^\perp$, the Hamming weight of $x \in \mathbb{F}_{q^k}^N$ is not smaller than d', and the i-th symbol $x_i \in \mathbb{F}_{q^k}$ of x is mapped to $\widetilde{y_i} \in C_1^{(i)}/C_2^{(i)\perp}$ for any $1 \le i \le N$ by $\widetilde{\pi_1}^{(i)}$. Since $\widetilde{y_i} \neq C_2^{(i)\perp}$ has Hamming weight not less than d_1, we have the assertion in the lemma. □

We can also prove the lemma without dealing directly with $\mathsf{d}_{\overline{C_2^\perp}}$.

Proof 2. For any $x \in D_1 \setminus D_2^\perp$, the Hamming weight of $x \in \mathbb{F}_{q^k}^N$ is not smaller than d', and x_i is mapped to y_i, a coset representative of $C_1^{(i)}/C_2^{(i)\perp}$ by $\pi_1^{(i)}$. If x_i is not zero, then y_i is not zero and hence, $\mathsf{w}(y_i + C_2^{(i)\perp}) \ge d_1$ by assumption (see (2)). Hence, we have the lemma. □

V. Bound on Minimum Distance

A. Geometric Goppa Codes for Outer Codes

We will seek for codes that exceed those in [8] or the non-CSS-type codes in [12], [13] in minimum distance for some region.

We use codes over $\mathbb{F}_{q^k}$, where $q^k = p^m$ with some p prime and m even, obtained from function fields of many rational places (places of degree one) as outer codes. Specifically, we use a sequence of function fields $F_\nu/\mathbb{F}_{q^k}$, $\nu = 1, 2, \ldots$, having genera g_ν and at least $N_\nu + 1$ rational places such that [15]

$$\lim_{\nu\to\infty} \frac{g_\nu}{N_\nu} = \gamma_k \stackrel{\text{def}}{=} \frac{1}{q^{k/2}-1}. \tag{4}$$

We put $A_\nu = P_1 + \cdots + P_{N_\nu}$, where P_i are distinct rational places in $F_\nu/\mathbb{F}_{q^k}$. Assume $G_{2,\nu}$ is a divisor of $F_\nu/\mathbb{F}_{q^k}$ having the form $G_{2,\nu} = m_2 P_\infty$, $m_2 < N_\nu$, with P_∞ being a rational place other than $P_1, \ldots, P_{N_\nu}$. Then, we have an $[N_\nu, K_{2,\nu}]$ code of minimum distance d'', where $K_{2,\nu} \ge \deg G_{2,\nu} + 1 - g_\nu$ and $d'' \ge N_\nu - \deg G_{2,\nu}$. We use this code as outer code D_2, and assume $D_1^\perp$ has a similar form. Specifically,

$$D_2 = C_{\mathcal{L}}(A_\nu, G_{2,\nu})$$

and

$$D_1 = C_{\mathcal{L}}(A_\nu, G_{1,\nu})^\perp,$$

where $G_{1,\nu} = m_1 P_\infty$ for some integer m_1, and

$$C_{\mathcal{L}}(A_\nu, G) = \big\{\big(f(P_1), \ldots, f(P_{N_\nu})\big) \mid f \in \mathcal{L}(G)\big\}.$$

Here, $\mathcal{L}(G) = \{x \in F_\nu \mid (x) \ge -G\} \cup \{0\}$, and (x) denotes the principal divisor of x (e.g., as in [16, p. 16]). We assume

$$G_{1,\nu} \le G_{2,\nu}$$

so that the CSS condition $D_1^\perp \le D_2$ is fulfilled.

We also assume

$$2g_\nu - 2 < \deg G_{j,\nu} < N_\nu, \quad j = 1, 2. \tag{5}$$

Then, the dimension of D_2 is

$$K_{2,\nu} = \dim G_{2,\nu} = \deg G_{2,\nu} - g_\nu + 1 \tag{6}$$

and that of D_1 is

$$K_{1,\nu} = N_\nu - \dim G_{1,\nu} = N_\nu - \deg G_{1,\nu} + g_\nu - 1. \tag{7}$$

The designed distance of D_2 is $N_\nu - \deg G_{2,\nu}$, and that of D_1 is $\deg G_{1,\nu} - 2g_\nu + 2$.

B. The Bound

With an invariant inner $[[n, k]]$ conjugate code pair (C_1, C_2) fixed, we consider an asymptotic situation where $K_{j,\nu}/N_\nu$ approaches a fixed rate R_j as ν goes to infinity ($j = 1, 2$). Note that the limit of $[K_{2,\nu} - (N_\nu - K_{1,\nu})]/N_\nu = (K_{1,\nu} + K_{2,\nu} - N_\nu)/N_\nu$, the information rate of the outer quotient codes, is given by

$$R_{\mathrm{q}} = R_1 + R_2 - 1. \tag{8}$$

Then, the overall rate of the concatenated conjugate code pair (L_1, L_2) has the limit

$$R_{\mathrm{o}} = \frac{k}{n} \lim_{\nu\to\infty} \frac{K_{1,\nu} + K_{2,\nu} - N_\nu}{N_\nu} = \frac{k}{n} R_{\mathrm{q}}. \tag{9}$$

If the quotient code $C_j/C_{\overline{j}}^\perp$, where $\overline{1} = 2$ and $\overline{2} = 1$, has minimum distance not smaller than d_j, we can bound the minimum distance $d_{\mathrm{o}}(j)$ of $L_j/L_{\overline{j}}^\perp$ using Lemma 2 as follows:

$$\begin{aligned} \liminf_{\nu\to\infty} \frac{d_{\mathrm{o}}(2)}{N_{\mathrm{o},\nu}} &\ge \frac{d_2}{n} \lim_{\nu\to\infty} \frac{N_\nu - \deg G_{2,\nu}}{N_\nu} \\ &= \frac{d_2}{n} \lim_{\nu\to\infty} \Big(1 - \frac{g_\nu}{N_\nu} - \frac{K_{2,\nu}}{N_\nu}\Big) \\ &= \frac{d_2}{n} \lim_{\nu\to\infty} \Big(1 - \frac{g_\nu}{N_\nu} - R_2\Big) \end{aligned} \tag{10}$$

by (6), and

$$\begin{aligned} \liminf_{\nu\to\infty} \frac{d_{\mathrm{o}}(1)}{N_{\mathrm{o},\nu}} &\ge \frac{d_1}{n} \lim_{\nu\to\infty} \frac{\deg G_{1,\nu} - 2g_\nu}{N_\nu} \\ &= \frac{d_1}{n} \lim_{\nu\to\infty} \Big(1 - \frac{g_\nu}{N_\nu} - R_1\Big) \end{aligned} \tag{11}$$

by (7). Note the asymptotic form of (5) is

$$\gamma_k \le R_j \le 1 - \gamma_k, \quad j = 1, 2. \tag{12}$$

It is expected that the best asymptotic bound will be obtained by requiring $d_1 d' \approx d_2 d''$, where d' and d'' are the minimum distances of the outer codes as in Lemma 2. Thus, we equalize the bound in (10) with that in (11), so that we have

$$d_1(1 - \gamma_k - R_1) = d_2(1 - \gamma_k - R_2).$$

Using this, (8) and (9), we can rewrite (10) and (11) as

$$\liminf_{\nu\to\infty} \frac{d_{\mathrm{o}}(j)}{N_{\mathrm{o},\nu}} \ge \frac{d_1 d_2}{n(d_1 + d_2)} \Big(1 - 2\gamma_k - \frac{n}{k} R_{\mathrm{o}}\Big) \tag{13}$$

for $j = 1, 2$. We summarize the above argument in the following theorem.

Theorem 2: Let a number $0 \le R \le 1$ be given. There exists a sequence of polynomially constructible $[[N_{\mathrm{o},\nu}, K_{\mathrm{o},\nu}, d_{\mathrm{o},\nu}]]$ conjugate code pairs that satisfies

$$\liminf_{\nu\to\infty} \frac{d_{\mathrm{o},\nu}}{N_{\mathrm{o},\nu}} \ge \sup \frac{d_1 d_2}{n(d_1+d_2)}\Big(1 - 2\gamma_k - \frac{n}{k}R\Big),$$

$\lim_{\nu\to\infty} K_{\mathrm{o},\nu}/N_{\mathrm{o},\nu} = R$, and $\lim_{\nu\to\infty} N_{\mathrm{o},\nu} = \infty$. Here, $\gamma_k = (q^{k/2}-1)^{-1}$, and the supremum is taken over all (n,k,d_1,d_2) such that an $[[n,k]]$ conjugate code pair (C_1,C_2) exists, $d_1 = \mathsf{w}(C_1 \setminus C_2^{\perp})$, $d_2 = \mathsf{w}(C_2 \setminus C_1^{\perp})$, and $q^k \ge 9$ is an even power of a prime.

Remarks. The polynomial constructibility of the sequence of conjugate code pairs, $\{(L_{1,\nu}, L_{2,\nu})\}$, is to be understood as the existence of a polynomial algorithm to produce a generator matrix G_ν of $L_{1,\nu}$ whose first $N_{\mathrm{o},\nu} - K_{2,\nu}$ rows span $L_{2,\nu}^{\perp}$ for each ν. Note such a generator matrix of $L_{1,\nu}$ can be converted into that of $L_{2,\nu}$ whose first $N_{\mathrm{o},\nu} - K_{1,\nu}$ rows span $L_{1,\nu}^{\perp}$ polynomially (see Fig. 1 of [5]; the conversion is done by calculating the inverse of an $N_{\mathrm{o},\nu} \times N_{\mathrm{o},\nu}$ matrix). Such a generator matrix G_ν specifies an encoder of the quotient code $L_{1,\nu}/L_{2,\nu}^{\perp}$, and a polynomial encoder of the corresponding quantum code [12] as well.

In our construction, the second Garcia-Stichtenoth tower of function fields was used [15]. See [17] for a polynomial algorithm to produce parity-check matrices of codes arising from the tower. □

VI. Calculable Bounds

First, we remark Theorem 2 recovers the bound of [8] by restricting the inner codes in the following manner. Assume C_1 is an $[n = 2t+1, k_1 = 2t, d_1 = 2]$ code such that $C_1^{\perp} = \mathsf{span}\, b_1$ with a fixed word $b_1 \in (\mathbb{F}_q \setminus \{0\})^n$, and C_2 is the $[n, k_2 = 2t+1, d_2 = 1]$ code, i.e., $\mathbb{F}_q^n$. Then, the substitution of the inner code parameters into (13) gives the following bound [8]:

$$l_t^{\mathrm{CLX}}(R_{\mathrm{o}}) = \frac{2}{3(2t+1)}\Big(1 - \frac{2}{q^t-1} - \frac{2t+1}{2t}R_{\mathrm{o}}\Big). \quad (14)$$

Theorem 2 also implies the bound in [9, Theorem 3.6]. Namely, if we put $n = k_1 = k_2 = d = 1$ and $C_1 = C_2 = \mathbb{F}_q^n$, we have

$$\liminf_{\nu\to\infty} \frac{d_{\mathrm{o},\nu}}{N_{\mathrm{o},\nu}} \ge l^{\mathrm{FLX}}(R) \stackrel{\mathrm{def}}{=} \frac{1}{2}\Big(1 - \frac{2}{\sqrt{q}-1} - R\Big). \quad (15)$$

Thus, the bound in Theorem 2 is not worse than the bounds in (14) and (15). We proceed to specifying an illustrative inner code pair, which results in a significant improvement.

Take two (not necessarily distinct) words $b_1, b_2 \in (\mathbb{F}_q \setminus \{0\})^n$ and set $C_j^{\perp} = \mathsf{span}\, b_j$, $j = 1,2$. We require the condition (1), i.e., $b_1 \cdot b_2 = 0$, and use the $[[n, n-2, 2]]$ conjugate code pair (C_1, C_2) as inner codes ($d_1 = d_2 = 2$). With this choice of the inner code pair, Theorem 2 immediately yields the following proposition, where we put $t = k/2 = (n-2)/2$.

Proposition 1: Let a number $0 \le R \le 1$ be given. There exists a sequence of polynomially constructible $[[N_{\mathrm{o},\nu}, K_{\mathrm{o},\nu}, d_{\mathrm{o},\nu}]]$ conjugate code pairs that satisfies

$$\liminf_{\nu\to\infty} \frac{d_{\mathrm{o},\nu}}{N_{\mathrm{o},\nu}} \ge \sup \frac{1}{t+1}\Big(\frac{1}{2} - \frac{1}{q^t-1} - \frac{t+1}{2t}R\Big),$$

$\lim_{\nu\to\infty} K_{\mathrm{o},\nu}/N_{\mathrm{o},\nu} = R$, and $\lim_{\nu\to\infty} N_{\mathrm{o},\nu} = \infty$. Here, the supremum is taken over t such that $q^t \ge 3$ is a power of a prime.

VII. Steane's Enlargement of CSS Codes

We digress to show that our approach also brings about an improvement on the known lower bound on the greatest minimum distance attainable by enlarged CSS codes [12], [13]. Enlarged CSS codes are a class of quantum error-correcting codes proposed by Steane [18]. These can be viewed as enlargements of conjugate code pairs (L_1, L_2) with $L_1 = L_2$, and are defined as follows. The definition below is general in that it applies to any prime power q. The concatenation of two vectors u, v will be denoted by $(u|v)$.

In essence, an $[[n,k]]$ symplectic quantum code (also known as a stabilizer code) can be viewed as a subspace of $\mathbb{F}_q^{2n}$ that contains its dual with respect to the standard symplectic bilinear form f_{sp} defined by $\mathsf{f}_{\mathrm{sp}}\big((u_x|u_z),(v_x|v_z)\big) = u_x \cdot v_z - u_z \cdot v_x$. Namely, when the subspace is spanned by the rows of a full-rank matrix of the form $\mathcal{G} = (G_x|\,G_z)$, where G_x and G_z are $(n+k)\times n$ matrices, G_x and G_z must satisfy

$$H_x G_z^{\mathrm{t}} - H_z G_x^{\mathrm{t}} = \mathbf{0} \quad (16)$$

for some $(n-k)\times 2n$ full-rank matrix $\mathcal{H} = (H_x|H_z)$ such that $\mathsf{span}\,\mathcal{H} \le \mathsf{span}\,\mathcal{G}$, where $\mathbf{0}$ denotes the zero vector, and $\mathsf{span}\, A$ denotes the space spanned by the rows of A. The space $\mathsf{span}\,\mathcal{H}$ is the dual of $\mathsf{span}\,\mathcal{G}$ with respect to f_{sp}.

Such an $(n+k)$-dimensional subspace may be called an f_{sp}-dual-containing code, but will be called an $[[n,k]]$ *symplectic code* for simplicity in this paper. It is well-known that a symplectic code over a finite field represents the essential structure of the corresponding symplectic quantum code, which is defined in terms of a unitary projective representation of $\mathbb{F}_q^{2n}$, e.g., [19], [20, Appendix A]. The minimum distance of a symplectic code generated by $\mathcal{G} = (G_x|G_z)$ as above is

$$\min\{\mathsf{w}([u,v]) \mid (u|v) \in \mathsf{span}\,\mathcal{G} \setminus \mathsf{span}\,\mathcal{H}\}$$

where $\mathsf{span}\,\mathcal{H}$ is the f_{sp}-dual of $\mathsf{span}\,\mathcal{G}$ as above, $[u,v]$ denotes $\big((u_1,v_1),\cdots,(u_{N_{\mathrm{o}}},v_{N_{\mathrm{o}}})\big) \in \mathcal{X}^{N_{\mathrm{o}}}$, $\mathcal{X} = \mathbb{F}_q^2$, for $u = (u_1,\ldots,u_{N_{\mathrm{o}}})$ and $v = (v_1,\ldots,v_{N_{\mathrm{o}}}) \in \mathbb{F}_q^{N_{\mathrm{o}}}$, and $\mathsf{w}([u,v])$ is the number of i with $(u_i,v_i) \ne (0,0)$.

Now we are ready to give a definition of Steane's enlargements of CSS codes. Assume we have an $[N_{\mathrm{o}}, K_{\mathrm{o}}]$ linear code C which contains its dual, $C^{\perp} \le C$, and which can be enlarged to an $[N_{\mathrm{o}}, K'_{\mathrm{o}}]$ linear code C'. Let a generator matrix W of C' has the form

$$W = \begin{pmatrix} U \\ V \end{pmatrix} \quad (17)$$

where U and V are of full rank, and U is a generator matrix of C, and let M be a $(K'_{\mathrm{o}} - K_{\mathrm{o}}) \times (K'_{\mathrm{o}} - K_{\mathrm{o}})$ invertible matrix. Then, the code generated by

$$\mathcal{G} = \left(\begin{array}{c|c} U & 0 \\ 0 & U \\ V & MV \end{array}\right) \quad (18)$$

is a symplectic code [18]. We denote this code by $\mathsf{S}(W,M)$. (Formally, we allow M to be '0×0 matrix.' In this case,

$C = C'$ and $\mathsf{S}(W, M)$ is the CSS code corresponding the conjugate code pair (C, C).)

Now suppose that $xM \neq \lambda x$ for any $\lambda \in \mathbb{F}_q$, i.e., that M is fixed-point-free when it acts on the projective space $(\mathbb{F}_q^{K'_{\rm o}-K_{\rm o}} \setminus \{\mathbf{0}\})/\sim$, where $x \sim y$ if and only if $y = \lambda x$ for some $\lambda \in \mathbb{F}_q$. This is possible by Lemma 4 in Appendix II if the size $K'-K$ of M is not less than 2. Such a choice of M results in a good symplectic code as the next lemma shows. This is a slight refinement of Theorem 1 of [18].

Lemma 3: Assume we have an $[N_{\rm o}, K_{\rm o}]$ linear code C which contains its dual, $C^\perp \leq C$, and which can be enlarged to an $[N_{\rm o}, K'_{\rm o}]$ linear code C', where $K'_{\rm o} \geq K_{\rm o}+2$. Take a full-rank generator matrix W of C' having the form in (17), where U is a generator matrix of C, and a fixed-point-free matrix M. Then, $\mathsf{S}(W, M)$ is an $[[N_{\rm o}, K_{\rm o}+K'_{\rm o}-N_{\rm o}, \geq \min\{d, d''\}]]$ symplectic code, where $d = \mathsf{w}(C \setminus C'^{\perp})$ and

$$d'' = \min\{\mathsf{w}([u, v]) \mid u, v \in C' \setminus C'^{\perp},\ \forall \lambda \in \mathbb{F}_q,\ v \neq \lambda u\}.$$

Corollary 1: Under the assumptions of the lemma, $\mathsf{S}(W, M)$ is an $[[N_{\rm o}, K_{\rm o}+K'_{\rm o}-N_{\rm o}, \geq \min\{d, d'_2\}]]$ symplectic code, where

$$d'_2 = \min\{\mathsf{w}([u, v]) \mid u, v \in C' \setminus \{\mathbf{0}\},\ \forall \lambda \in \mathbb{F}_q,\ v \neq \lambda u\}.$$

Corollary 2: Under the assumptions of the lemma, $\mathsf{S}(W, M)$ is an $[[N_{\rm o}, K_{\rm o} + K'_{\rm o} - N_{\rm o}, \geq \min\{d, \lceil \frac{q+1}{q} d' \rceil\}]]$ symplectic code, where $d' = \mathsf{w}(C' \setminus C'^{\perp})$.

Remarks. The premise of the lemma implies

$$C'^{\perp} \leq C^{\perp} \leq C \leq C'. \tag{19}$$

In Steane's original bound [18, Theorem 1], $\mathsf{w}(C \setminus \{\mathbf{0}\})$ and $\mathsf{w}(C' \setminus \{\mathbf{0}\})$ were used in place of $d = \mathsf{w}(C \setminus C'^{\perp})$ and $d' = \mathsf{w}(C' \setminus C'^{\perp})$, respectively. The quantity d'_2, which is implicit in Steane's original proof, is the second generalized Hamming weight of C' as pointed out in [21]. □

To prove Lemma 3 and corollaries, we should only examine the proof of Theorem 1 in [18] noting that we may assume H', the generator matrix of $C'^{\perp}$, is a submatrix of U (G in [18]). In particular, if $q = 2$, this can be done without pain. A proof for the general prime power q is included in Appendix II.

In [12], Steane's construction was applied to binary expansions of geometric Goppa codes $D^\perp \leq D \leq D'$. The binary expansion of a code D_1 over $\mathbb{F}_{q^k}$ denotes $\pi_1(D_1)$ with $n = k$ and $q = 2$ in our notation (Section IV and [5]), where the inner code is the trivial $[[n, n]]$ code. They also assume $\pi_1 = \pi_2$, which is possible by use of self-dual bases of $\mathbb{F}_{q^k}$ [5]. In [13], it was observed how the bound in [12] increases if their geometric Goppa codes were replaced by another sequence of geometric Goppa codes that use almost all rational places of the underlying function fields.

In what follows, we establish a similar bound for the case where the $[[n, n]]$ inner code pair $(\mathbb{F}_{q^k}, \mathbb{F}_{q^k})$ is replaced by a general $[[n, k]]$ inner code pair (C_1, C_2) with $C_1 = C_2$.

The main ingredient of the construction in [12], [13] is a tower of codes $D^\perp \leq D \leq D'$ over $\mathbb{F}_{q^k}$, all of which arise from some sequence of function fields $F_1, F_2, \cdots$, such as given in [22], and have the form

$$C_{\mathcal{L}}(A_\nu, G) = \big\{\big(f(P_1), \ldots, f(P_N)\big) \mid f \in \mathcal{L}(G)\big\}.$$

Specifically,

$$D = C_{\mathcal{L}}(A_\nu, G), \quad D' = C_{\mathcal{L}}(A_\nu, G'),$$

where $A_\nu = P_1 + \cdots + P_N$, P_i are distinct rational places in $F_\nu/\mathbb{F}_{q^k}$, and G, G' are divisors of $F_\nu/\mathbb{F}_{q^k}$ whose supports are disjoint with that of A_ν. Put $\lim_\nu g_\nu/N = \hat{\gamma}$. The best possible case is that $\hat{\gamma} = \gamma_k$ if q^k is a square as in Section V. The major difficulty of the construction resides in the constraint $D^\perp \leq D \leq D'$, i.e., $G^\perp \leq G \leq G'$ when $D^\perp$ is written as $C_{\mathcal{L}}(A_\nu, G^\perp)$.

In our construction, we apply Lemma 3 assuming $C = \pi_1(D) + \overline{C_1^\perp}$ and $C' = \pi_1(D') + \overline{C_1^\perp}$, where π_1 and $\overline{C_1^\perp}$ are as in [5, Section III] or in Section IV of the present paper. We also assume $\pi_1 = \pi_2$. Since $C_1 = C_2$, Theorem 1 implies $C^\perp = \pi_1(D^\perp) + \overline{C_1^\perp}$ and $C'^\perp = \pi_1(D'^\perp) + \overline{C_1^\perp}$. Namely, in the present case, the tower in (19) can be written as

$$\pi_1(D'^\perp) + B \leq \pi_1(D^\perp) + B \leq \pi_1(D) + B \leq \pi_1(D') + B \tag{20}$$

where $B = \overline{C_1^\perp} = \bigoplus_{i=1}^N C_1^\perp$. Keeping in mind evaluating d_B, rather than d, is enough for our purpose, one can calculate the bound almost the same way as in [12], which leads to the next proposition. A proof may be found in Appendix II.

Proposition 2: Suppose either q is even or both q and k are odd. Assume further that we have an $[[n, k, \geq d]]$ conjugate code pair (C_1, C_2) with $C_1 = C_2$ over $\mathbb{F}_q$, a sequence of function fields $\{F_\nu/\mathbb{F}_{q^k}\}$ and a sequence of positive integers $\{N_\nu\}$ with $N_\nu \to \infty$ ($\nu \to \infty$) satisfying the following three conditions for any $R' > R \geq 1/2$. (i) For all large enough ν, we have $N = N_\nu$ distinct rational places $P_1, \cdots, P_N$ in $F_\nu/\mathbb{F}_{q^k}$, and divisors $G = G_\nu$ and $G' = G'_\nu$ of $F_\nu/\mathbb{F}_{q^k}$ such that (a) the supports of G, G' contain none of $P_1, \cdots, P_N$, (b) $G \leq G'$, and (c) $D^\perp \leq D$ for $D = C_{\mathcal{L}}(A, G)$, where $A = P_1 + \cdots + P_N$. (ii) The genus g_ν of $F_\nu/\mathbb{F}_{q^k}$ satisfies

$$\hat{\gamma} \stackrel{\rm def}{=} \lim_{\nu\to\infty} \frac{g_\nu}{N} < \frac{1}{2}.$$

(iii) G and G' fulfill

$$\lim_{\nu\to\infty} \frac{\deg G - g_\nu}{N} = R, \quad \lim_{\nu\to\infty} \frac{\deg G' - g_\nu}{N} = R'.$$

Then, we have a sequence of $[[N_{\rm o}, K''_{\rm o}, d_{\rm o}]]$ symplectic codes $\mathsf{S}(W_\nu, M_\nu)$ that satisfies $\lim_\nu N_{\rm o} = \infty$,

$$\liminf_{\nu\to\infty} \frac{K''_{\rm o}}{N_{\rm o}} \geq R_{\rm o}$$

and

$$\liminf_{\nu\to\infty} \frac{d_{\rm o}}{N_{\rm o}} \geq \frac{(q+1)d}{2q+1}\Big(\frac{1-2\hat{\gamma}}{n} - \frac{1}{k}R_{\rm o}\Big)$$

for any

$$R_{\rm o} \geq \frac{k}{2(q+1)n}(1-2\hat{\gamma}).$$

Remark. The assumption that for any $R' > R \geq 1/2$, (iii) holds says $\deg G$ and $\deg G'$ are flexible enough (the

dimension of D is $\deg G - g_\nu + 1$, and $R \geq 1/2$ stems from $D^\perp \leq D$). This, as well as the other two, is fulfilled, e.g., if the chosen outer codes are from [13], [23], [24]. □

This recovers the bound in [12] by putting $\hat{\gamma} = (\gamma_k^{-1} - 1)^{-1}$, $q = 2$, $n = k = 2m$ and $d = 1$, as well as that in [13] by putting $\hat{\gamma} = \gamma_k$ and using the same q, n, k, d.

If the inner code is the same as in Proposition 1, and the outer codes attain $\hat{\gamma} = \gamma_{2t}$, where $q = 2$, the constructed $[[N_{\rm o}, K''_{\rm o}, d_{\rm o}]]$ symplectic codes satisfy

$$\liminf_{\nu\to\infty} \frac{K''_{\rm o}}{N_{\rm o}} \geq R_{\rm o}$$

and

$$\liminf_{\nu\to\infty} \frac{d_{\rm o}}{N_{\rm o}} \geq \frac{3}{5(t+1)}(1 - 2\gamma_{2t}) - \frac{3}{5t} R_{\rm o} \tag{21}$$

where

$$R_{\rm o} \geq \frac{t}{6(t+1)}(1 - 2\gamma_{2t}). \tag{22}$$

VIII. Comparisons

In this section, we will compare the bound in Proposition 1 with that in [8] for conjugate code pairs (CSS codes), and the bound (21) with that in [13] for enlarged CSS codes. Note that the codes in [13] exceed the original constructible quantum codes [12] everywhere in relative minimum distance.

Let a point (δ, R) be called attainable if we have a sequence of polynomially constructible $[[N_\nu, K_\nu, d_\nu]]$ conjugate codes $(C_{1,\nu}, C_{2,\nu})$ such that $\liminf_\nu d_\nu/N_\nu \geq \delta$, $\liminf_\nu K_\nu/N_\nu \geq R$, and $\lim_\nu N_\nu = \infty$. Then, Proposition 1 states that the points in $\bigcup_{t\geq 3} \mathcal{M}_t$ is attainable, where

$$\mathcal{M}_t = \{(\delta, R) \mid 0 \leq \delta \leq 1 \text{ and } 0 \leq R \leq R_t(\delta)\} \tag{23}$$

and

$$R_t(\delta) = \frac{t}{t+1}\Big(1 - \frac{2}{q^t - 1}\Big) - 2t\delta. \tag{24}$$

Note $R = R_t(\delta)$ is merely a rewriting of

$$\delta = l_t(R) \stackrel{\rm def}{=} \frac{1}{t+1}\Big(\frac{1}{2} - \frac{1}{q^t - 1} - \frac{t+1}{2t} R\Big).$$

Hence, our bound is the upper boundary of the region $\bigcup_{t\geq 3} \mathcal{M}_t$, which is the envelope formed by the collection of the straight lines $R = R_t(\delta)$, $t \geq 3$.

Let δ_t be the solution of $R_t(\delta) = R_{t+1}(\delta)$ for $t = 3, 4, \cdots$, and let δ_2 be the solution of $R_3(\delta) = 0$. Then, the upper envelope is the broken lines obtained by connecting the points $(\delta_t, R_{t+1}(\delta_t))$, $t = 2, 3, \cdots$. The four bounds to be compared below are all represented similarly as broken lines. For example, denoting by $R_t^{\rm CLX}$ the inverse of $l_t^{\rm CLX}$ defined in (14), and using $R_t^{\rm CLX}$ in place of R_t, we have the broken lines representing the bound in [8].

These bounds are plotted in Fig. 1. The improvement is clear from the figure. In fact, we can show the bound in Proposition 1 exceeds that in [8] for $\delta > \delta^* \approx 0.00734$, where δ^* denotes the solution of $R_8(\delta) = R_7^{\rm CLX}(\delta)$. Similarly, the bound for enlarged CSS codes in (21) exceeds that in [13] for $\delta > 2339/157480 \approx 0.0149$.

In the comparisons above, we have assumed $q = 2$. It was observed in [9] that the bound in (15) is larger than

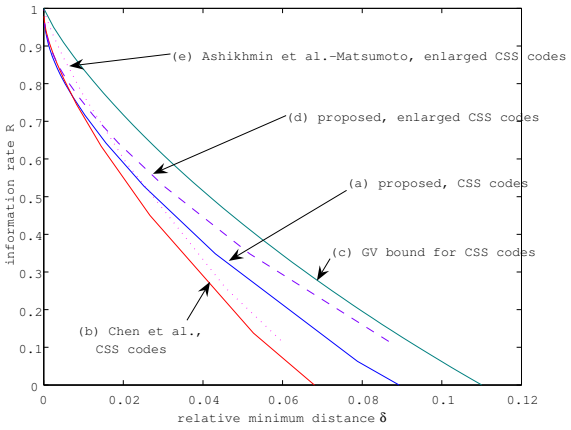

Fig. 1. Bounds on the minimum distance of binary CSS and enlarged CSS codes. The plotted bounds are (a) the improved bound on the minimum distance of concatenated conjugate codes (CSS codes) in Proposition 1, (b) the bound attainable by the CSS codes of Chen, Ling and Xing [8], (c) the Gilbert-Varshamov-type bound $R = 1 - 2H_2(\delta)$ for CSS codes [1], where H_2 is the binary entropy function, (d) the bound attainable by the enlarged CSS quantum codes in (21), and (e) that in [13].

the quantum Gilbert-Varshamov bound in some range of R for $q \geq 19^2$, as the Tsfasman-Vlăduţ-Zink bound is larger than the classical Gilbert-Varshamov bound for $q \geq 49$. In [9, Theorem 3.8], they also presented the bound

$$R^{\rm FLX2}(\delta) \stackrel{\rm def}{=} 1 - \frac{2}{\sqrt{q} - 1} + \log_q(1 + q^{-3}) - 2\delta,$$

which is attainable by non-symplectic quantum codes and improves slightly on the bound in (15). The bound in Proposition 1 is sometimes better than $R^{\rm FLX2}(\delta)$. For example, when $3 \leq q \leq 19$, we have $R_1(\delta) \geq R^{\rm FLX2}(\delta)$ for any δ, which implies $\sup_t R_t(\delta) \geq R^{\rm FLX2}(\delta)$. Proposition 2 with $n = k = 1$ and $\hat{\gamma} = \gamma_k = (\sqrt{q} - 1)^{-1}$ improves, although slightly, on $R^{\rm FLX2}(\delta)$ for $(q+1)\log_q(1+q^{-3}) < \delta \leq 1/2 - \hat{\gamma}$ when $q \geq 16$.

IX. Summary and Remark

The minimum distance of concatenated conjugate codes was evaluated to demonstrate that this class contains codes superior to those previously known.

For the quotient codes C/B obtained by means of concatenation in this work, the minimum distance $\mathsf{d}_B(C) = \mathsf{w}(C \setminus B)$ of C/B is significantly larger than the usual minimum distance $\mathsf{w}(C \setminus \{\mathbf{0}\})$ of C. In fact, B contains the space of the form $\bigoplus_{i=1}^N C_1^\perp$, which implies $\mathsf{w}(C \setminus \{\mathbf{0}\})/N_{\rm o} \leq 1$, where $N_{\rm o}$ is the length of C. It was demonstrated that the underlying metric structure, d_B, plays a role in evaluating $\mathsf{w}(C \setminus B)$.

Appendix I
Other Bounds

A. Zyablov-type bound

In this section, we will prove a bound similar to the Zyablov bound (e.g., [25, p. 315]): For some polynomially constructible

$[[N_{\rm o}, K_{\rm o}]]$ concatenated conjugate code pairs, we have

$$\limsup_{N_{\rm o}\to\infty} \frac{d_{\rm o}}{N_{\rm o}} \geq \frac{1}{2} \max_{rR=R_{\rm o}} \Big[(1-R)H_q^{-1}\Big(\frac{1-r}{2}\Big)\Big] \qquad (25)$$

where the maximum is taken over $\{(r,R) \mid 0 \leq r \leq 1, 0 \leq R \leq 1, rR = R_{\rm o}\}$, $K_{\rm o}/N_{\rm o}$ approaches $R_{\rm o}$ as $N_{\rm o} \to \infty$, and H_q^{-1} is the inverse of the function H_q defined by

$$H_q(x) = x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$$

for $0 < x \leq (q-1)/q$ and $H_q(0) = 0$.

Proof of (25). This bound is achieved by the following concatenation of codes. We employ an inner conjugate code pair achieving the Gilbert-Varshamov-type bound [1] (also [26] and Section B below) and the $[N, K_1 = K_2]$ generalized Reed-Solomon (GRS) outer codes. Namely, the outer code pair (D_1, D_2) is such that both D_1 and D_2 are GRS codes of the same dimension. We consider an asymptotic situation where both N and n go to infinity, $R_{\rm c} = K_1/N$ approaches a fixed rate $R_{\rm c}^*$, and $r_{\rm c} = k_1/n = k_2/n$ approaches a rate $r_{\rm c}^*$. The inner conjugate code pairs (C_1, C_2) are such that $d_1 = \mathsf{d}_{C_2^\perp}(C_1)$ and $d_2 = \mathsf{d}_{C_1^\perp}(C_2)$ are bounded by $\liminf_{n\to\infty} \min\{d_1, d_2\}/n \geq H_q^{-1}(1-r_{\rm c}^*)$ (see Section I-B below).

Let d, d' and $d_{\rm o}$ denote the minimum distance of the inner code $\min\{d_1, d_2\}$, that of the outer codes, that of the concatenated conjugate code, respectively. Then, $d_{\rm o} = dd'$ by Lemma 2. Putting $N_{\rm o} = nN$, we have

$$\limsup_{N_{\rm o}\to\infty} \frac{d_{\rm o}}{N_{\rm o}} \geq (1-R_{\rm c}^*)H_q^{-1}(1-r_{\rm c}^*).$$

Converting the rates $R_{\rm c} \to R_{\rm c}^*$ and $r_{\rm c} \to r_{\rm c}^*$ into those of quotient codes $k/n \to r$ and $K/N \to R$ by $r_{\rm c}^* = (r+1)/2$, which stems from $k = k_1 + k_2 - n = 2k_1 - n$, and $R_{\rm c}^* = (R+1)/2$, we have (25) for the concatenated conjugate codes of asymptotic rate $R_{\rm o}$.

B. Gilbert-Varshamov-type bound

We have remarked [26, p. 8310] that the Gilbert-Varshamov-type (GV) bound for conjugate codes (CSS codes), non-constructible in general, follows from a more general bound on the spectrum of codes. We will give a proof of this remark in this section.

In [26], [6], it was shown that there exists a conjugate code pair consisting of an $[n, r_1 n]$ code C_1 and an $[n, r_2 n]$ code C_2 such that

$$M_Q(C_j \setminus C_{\overline{j}}^\perp) \leq a_n |\mathcal{T}_Q^n| q^{-n(1-r_j)}, \quad Q \in \mathcal{P}_n(\mathbb{F}_q) \qquad (26)$$

for $j = 1, 2$, where $\mathcal{P}_n(\mathbb{F}_q)$ is the set of n-types and $M_Q(C)$ is the number of words having type Q in C (for preciseness, see [26], [3]), $\overline{1} = 2$, $\overline{2} = 1$, and a_n is a positive number at most polynomial in n. The list of numbers $(M_Q(C))_{Q\in\mathcal{P}_n(\mathbb{F}_q)}$ may be called the spectrum, or P-spectrum, of C.

From (26) and $|\mathcal{T}_Q^n| \leq q^{nH(Q)}$, where H denotes the entropy, it immediately follows that $M_Q(C_j \setminus C_{\overline{j}}^\perp) = 0$ if $1 - r_j - H(Q) - (\log_q a_n)/n > 0$. Hence, $H(\mathsf{P}_y) \geq 1 - r_j - (\log_q a_n)/n$ for any word $x \in C_j \setminus C_{\overline{j}}^\perp$, where P_y denotes the type of y. But $H_q(\mathsf{w}(y)/n) \geq H(\mathsf{P}_y)$ for any $y \in \mathbb{F}_q^n$ if we extend H_q by $H_q(x) = 1$ for $(q-1)/q < x \leq 1$. Hence, we have $H_q(d_j/n) \geq 1 - r_j - (\log_q a_n)/n$. Setting $r_1 = r_2$, and denoting the rate of the conjugate code pair (C_1, C_2) or the corresponding CSS code by $r = r_1 + r_2 - 1$, we have

$$r \geq 1 - 2H_q(\min\{d_1, d_2\}/n) - 2(\log_q a_n)/n. \qquad (27)$$

This is the GV bound for CSS codes.

Note what is often called the quantum Gilbert-Varshamov bound has the form $R = 1 - 2H_{q^2}(\delta)$ and this is larger than the GV bound for CSS codes $R = 1 - 2H_q(\delta)$.

Appendix II
Proofs for Enlarged CSS Codes

A. Proof of Lemma 3

First, we show the existence of a needed fixed-point-free matrix. Note that a fixed-point-free matrix is a paraphrase of a matrix having no eigenvalue in $\mathbb{F}_q$.

Lemma 4: Let $a(x) = x^m - a_m x^{m-1} \cdots - a_2 x - a_1$ be an irreducible polynomial over $\mathbb{F}_q$, where $m \geq 2$. Then, the matrix

$$M = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & \cdots & & \\ 0 & 0 & 0 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_m \end{pmatrix} \qquad (28)$$

has no eigenvalue in $\mathbb{F}_q$.

Remark. Either M or its transpose $M^{\rm t}$ is called the companion matrix of $a(x)$.

Proof 1. The characteristic polynomial of M is $a(x)$ itself as can be checked by a direct calculation. Hence, M has no eigenvalue in $\mathbb{F}_q$. □

Proof 2. Let α be a root of $a(x)$. Then, putting $\varphi(\xi) = (\xi_1, \ldots, \xi_m)$ for $\xi = \xi_1 + \xi_2\alpha + \cdots + \xi_m\alpha^{m-1} \in \mathbb{F}_{q^m}$, we have $\varphi(\alpha^i)M = \varphi(\alpha^{i+1})$ (see, e.g., [5, Appendix]). But $\varphi(\alpha^i) \sim \varphi(\alpha^j)$ occurs only if α^{j-i} is in the subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^m}$, while α is not in $\mathbb{F}_q$. Hence, M is fixed-point-free, i.e., it has no eigenvalue in $\mathbb{F}_q$. □

The following corollary is trivial.

Corollary 3: For any prime q and $m \geq 2$, there exists an $m \times m$ invertible matrix having no eigenvalue in $\mathbb{F}_q$.

Proof of Lemma 3 and its corollaries. We should only prove the bound on minimum distance since the other part of the proof of [18] is valid for any prime power q.

Denoting a generator matrix of $C'^\perp$ by H', we may assume H' is a submatrix of the generator matrix U of $C^\perp$. Then, since $\mathsf{span}\,\mathcal{H} \leq \mathsf{span}\,\mathcal{G}$, we may assume

$$\mathcal{H}' = \left(\begin{array}{c|c} H' & 0 \\ 0 & H' \end{array}\right)$$

is a submatrix of the 'stabilizer' matrix $\mathcal{H}$, as shown in [18], and hence is a submatrix of $\mathcal{G}$ as well.

We consider $\mathsf{w}([u,v])$ for $x = (u|v) \in \mathsf{span}\,\mathcal{G} \setminus \mathsf{span}\,\mathcal{H}'$, noting $\mathsf{span}\,\mathcal{H}' = C'^\perp \oplus C'^\perp$. If no rows of $(V|MV)$ are involved in the generation of $(u|v)$, then $\mathsf{w}([u,v]) \geq d$. Note, otherwise, $u, v \in C' \setminus C'^\perp$ and $v \neq \lambda u$ for any λ. Hence, we have the lemma.

Corollary 1 is trivial. We establish Corollary 2 by proving $d'' \ge \lceil \frac{q+1}{q} d' \rceil$. Namely, we show that for any pair of linearly independent vectors $u, v \in C' \setminus C'^{\perp}$, we have $\mathsf{w}([u,v]) \ge \lceil \frac{q+1}{q} d' \rceil$. Write $u = (u_1, \ldots, u_{N_\mathrm{o}})$, $v = (v_1, \ldots, v_{N_\mathrm{o}})$, and put $w = \mathsf{w}(u)$. Without loss of generality, we may assume $u_{w+1} = \cdots = u_{N_\mathrm{o}} = 0$. Denoting the number of i with $v_i = \lambda u_i$, $1 \le i \le w$, by $l(\lambda)$ for $\lambda \in \mathbb{F}_q$, we have an element $\lambda^* \in \mathbb{F}_q$ with $l(\lambda^*) \ge w/q$, the average of $l(\lambda)$. Then,

$$d' \le \mathsf{w}(v - \lambda^* u) \le w - \frac{w}{q} + \mathsf{w}\big((v_{w+1}, \ldots, v_{N_\mathrm{o}})\big).$$

Hence, we have $\mathsf{w}([u,v]) = w + \mathsf{w}\big((v_{w+1}, \ldots, v_{N_\mathrm{o}})\big) \ge d' + w/q \ge d'(1 + 1/q)$, and the corollary. □

B. Proof of Proposition 2

In our construction, we apply Lemma 3 assuming the tower in (19) is that in (20). Note $\dim C_1^{\perp} = (n-k)/2$, which follows from that $C_1/C_2^{\perp}$ is an $[[n,k]]$ quotient code and $C_1 = C_2$, and hence,

$$N_\mathrm{o} = nN, \quad K_\mathrm{o} = kK + \frac{n-k}{2}N,$$
$$K'_\mathrm{o} = kK' + \frac{n-k}{2}N$$

where

$$K = \dim_{\mathbb{F}_{q^k}} D, \quad K' = \dim_{\mathbb{F}_{q^k}} D'.$$

Hence, the overall rate of the quantum code is

$$\frac{K_\mathrm{o} + K'_\mathrm{o} - N_\mathrm{o}}{N_\mathrm{o}} = \frac{k}{n}\Big(\frac{K+K'}{N} - 1\Big). \tag{29}$$

Put

$$\delta = \liminf_{\nu\to\infty} \frac{\mathsf{w}(\pi_1(D) \setminus B)}{N_\mathrm{o}}, \quad \delta' = \liminf_{\nu\to\infty} \frac{\mathsf{w}(\pi_1(D') \setminus B)}{N_\mathrm{o}}.$$

Then, the analysis in Section V that leads to (10) and (11), which actually lower-bounds the minimum distance of the concatenation of $C_j/C_j^{\perp}$ and $D_j/\{\mathbf{0}\} = D_j$, gives

$$\delta \ge \frac{d}{n}(1 - \hat{\gamma} - R) \stackrel{\mathrm{def}}{=} a, \quad \delta' \ge \frac{d}{n}(1 - \hat{\gamma} - R') \stackrel{\mathrm{def}}{=} a'$$

where R, R' are the limits appearing in the condition (iii).

Putting

$$R'' = R + R' - 1 \ \text{ and } \ a = a'(q+1)/q, \tag{30}$$

we have

$$\min\{\delta, \delta'(q+1)/q\} \ge \frac{(q+1)d}{(2q+1)n}(1 - 2\hat{\gamma} - R'').$$

Then, noting (29) and

$$\liminf_{\nu\to\infty} \frac{K}{N} \ge R, \quad \liminf_{\nu\to\infty} \frac{K'}{N} \ge R',$$

which imply

$$\liminf_{\nu\to\infty} \frac{K+K'}{N} - 1 \ge R'',$$

we see the overall rate of the quantum code satisfies

$$\liminf_{\nu\to\infty} \frac{K_\mathrm{o} + K'_\mathrm{o} - N_\mathrm{o}}{N_\mathrm{o}} \ge \frac{k}{n} R'' = R_\mathrm{o}.$$

Thus, the constructed $[[N_\mathrm{o}, K''_\mathrm{o}, d_\mathrm{o}]]$ quantum codes satisfy

$$\liminf_{\nu\to\infty} \frac{K''_\mathrm{o}}{N_\mathrm{o}} \ge R_\mathrm{o} \tag{31}$$

and

$$\liminf_{\nu\to\infty} \frac{d_\mathrm{o}}{N_\mathrm{o}} \ge \frac{(q+1)d}{2q+1}\Big(\frac{1-2\hat{\gamma}}{n} - \frac{1}{k}R_\mathrm{o}\Big) \tag{32}$$

by Corollary 2. Note (32) can be attained for any

$$R_\mathrm{o} \ge \frac{k}{2(q+1)n}(1 - 2\hat{\gamma}), \tag{33}$$

which is a rewriting of $R \ge 1/2$. (Given R_o, put $R'' = nR_\mathrm{o}/k$ and let (R, R') be the solution of (30); see also the remark to the proposition.)

Noting $\mathbb{F}_{q^k}$ has a self-dual basis over $\mathbb{F}_q$ if and only if either q is even or both q and k are odd [27] (also [28, p. 75] for the statement only), we have the proposition.

REFERENCES

[1] A. R. Calderbank and P. W. Shor, "Good quantum error correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 1996.

[2] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. Roy. Soc. Lond. A*, vol. 452, pp. 2551–2577, 1996.

[3] M. Hamada, "Quotient codes and their reliability," *IPSJ Digital Courier*, vol. 1, pp. 450–460, Oct. 2005. Available at `http://www.jstage.jst.go.jp/article/ipsjdc/1/0/1_450/_articl` Also appeared in *IPSJ Journal*, vol. 46, pp. 2428–2438, no. 10, Oct., 2005.

[4] P. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, July 2000.

[5] M. Hamada, "Concatenated conjugate codes," submitted to *IEEE Trans. Information Theory*, Aug. 2006.

[6] M. Hamada, "Constructive conjugate codes achieving high rates" (tentative), 2006. Manuscript in preparation.

[7] S. G. Vléduts, G. L. Katsman, and M. A. Tsfasman, "Modular curves and codes with polynomial complexity of construction," *Problems of Information Transmission*, vol. 20, no. 1, pp. 35–42, 1984.

[8] H. Chen, S. Ling, and C. Xing, "Asymptotically good quantum codes exceeding the Ashikhimin-Litsyn-Tsfasman bound," *IEEE Trans. Information Theory*, vol. 47, pp. 2055–2058, July 2001.

[9] K. Feng, S. Ling, and C. Xing, "Asymptotic bounds on quantum codes from algebraic geometry codes," *IEEE Trans. Information Theory*, vol. 52, pp. 986–991, Mar. 2006.

[10] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*. Boston: Kluwer, 1991.

[11] S. A. Stepanov, *Codes on Algebraic Curves*. New York: Kluwer/Plenum, 1999.

[12] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," *Phys. Rev. A*, vol. 63, pp. 032311–1–5, 2001.

[13] R. Matsumoto, "Improvement of Ashikhimin-Litsyn-Tsfasman bound for quantum codes," *IEEE Trans. Information Theory*, vol. 48, pp. 2122–2124, July 2002.

[14] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[15] A. Garcia and H. Stichtenoth, "On the asymptotic behaviour of some towers of function fields over finite fields," *Journal of Number Theory*, vol. 61, p. 248–273, 1996.

[16] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin: Springer-Verlag, 1993.

[17] K. W. Shum, I. Aleshnikov, P. V. Kumar, H. Stichtenoth, and V. Deolalikar, "A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound," *IEEE Trans. Information Theory*, vol. 47, pp. 2225–2241, Sept. 2001.

[18] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Trans. Information Theory*, vol. 45, pp. 2492–2495, Nov. 1999.

[19] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Information Theory*, vol. 47, pp. 3065–3072, Nov. 2001.

[20] M. Hamada, "Notes on the fidelity of symplectic quantum error-correcting codes," *International Journal of Quantum Information*, vol. 1, no. 4, pp. 443–463, 2003.
[21] G. Cohen, S. Encheva, and S. Litsyn, "On binary constructions of quantum codes," *IEEE Trans. Information Theory*, vol. 45, pp. 2495–2498, Nov. 1999.
[22] A. Garcia and H. Stichtenoth, "A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound," *Inventions mathematicae*, vol. 121, pp. 211–222, 1995.
[23] H. Stichtenoth, "Transitive and self-dual codes attaining the Tsfasman-Vlăduţ-Zink bound," *IEEE Trans. Information Theory*, vol. 52, pp. 2218–2224, May 2006.
[24] C. Voss and T. Høholdt, "An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound the fist step," *IEEE Trans. Information Theory*, vol. 43, pp. 128–135, Jan. 1997.
[25] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. NY: North-Holland, 1977.
[26] M. Hamada, "Reliability of Calderbank-Shor-Steane codes and security of quantum key distribution," *J. Phys. A: Math. Gen.*, vol. 37, pp. 8303–8328, 2004. E-Print, quant-ph/0308029, LANL, 2003.
[27] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," *SIAM J. Comput.*, vol. 9, pp. 759–767, Nov. 1980.
[28] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge: Cambridge University Press, 2nd ed., 1997.